REGULATORY FRAMEWORK OF DATA BREACHES IN THE INDIAN BANKING SECTOR

Arisha Khan, BA LLB (H), Amity Law School, Noida

ABSTRACT

The security and confidentiality of sensitive information are seriously threatened by data breaches, especially in sectors like banking that handle enormous volumes of personal and financial data. This article explores the legal structure that controls data breaches in the Indian banking industry. An overview of the growing dependence of banking operations on digital infrastructure and the resulting susceptibilities to cyberattacks and data breaches is given in the introduction. It emphasizes how crucial strong regulatory frameworks are to reducing these risks and preserving consumer confidence.

The study examines important laws and policies concerning data breaches in the Indian banking industry. It examines the Reserve Bank of India's (RBI) policies and directives on data protection, cybersecurity, and incident reporting procedures, as well as the Information Technology Act, of 2000, and its updates. It also looks at other laws that are pertinent and how they affect financial organizations. Moreover, the study delineates the functions and accountabilities of regulatory entities supervising cybersecurity and data protection within the Indian banking industry. Along with the functions of other agencies like the Ministry of Electronics and Information Technology (MeitY) and the Data Protection Authority (DPA) suggested under the Personal Data Protection Bill, it examines the crucial role of the RBI as the main regulator.

The study concludes by analyzing the fines and repercussions associated with the Indian banking sector's noncompliance with data breach laws. It evaluates the potential financial penalties, legal ramifications, and harm to banks' reputations that might result from their noncompliance with regulatory requirements. It also covers how data breach events affect market stability, customer trust, and regulatory control. As a result, the study emphasizes how critical it is to have a thorough regulatory framework in place to deal with data breaches in the Indian banking industry. In order to ensure the resilience and integrity of the financial ecosystem, it highlights the necessity of continuously enhancing and adapting rules to keep up with the rapid improvements in technology and growing cyber threats.

INTRODUCTION

Data security has become the cornerstone of trust in the banking industry in the digital era, as sensitive information flows smoothly across networks and financial transactions happen at the touch of a button. The banking sector in India is a vital data steward as well as a desirable target because of its enormous client base and complex financial activities. It is critical that we comprehend the importance of data security and the growing risks posed by cyberspace as we embrace digitization. This comprehensive paper delves into the complex realm of data protection in Indian banks, examining its significance, the dynamic threat landscape, and methods to secure sensitive data.

In banking, trust is the currency. Banks get the financial assets, personal information, and transaction records that belong to their customers. Any betrayal of this trust might have dire repercussions, damaging the institution's reputation and undermining consumer confidence. Strong data security is essential for establishing confidence with clients as well as being a legal need.

Banking and the financial sector are high-stakes businesses. Taking into account the following:

- *Monetary Losses*: If a cyberattack is successful, the bank and its clients may suffer large financial losses. The financial line is immediately impacted by fraudulent transactions, lost money, and operational interruptions.

- *Economic Stability*: Because financial systems are interrelated, a breach in one organization can have a cascading effect on others. The whole financial ecosystem is upended by a compromised bank, which has an impact on investors, companies, and the overall economy.

- *Regulatory Scrutiny*: Data security procedures are regularly inspected by regulatory organizations. Juvenile penalties, legal disputes, and reputational harm can result from noncompliance.

India is dealing with an increasingly dangerous cyber environment.

- *Information Breach*: Indian banks have revealed that between June 2018 and March

2022, there were 248 significant breaches of information by cybercriminals. The attack surface has grown due to the increase in digital transactions and connectivity.

- *Rise in Ransomware assaults*: Financial services have seen an increase in ransomware assaults, which interrupt operations and demand large ransom payments.

- *Distributed Denial of Service (DDoS) assaults*: DDoS assaults overload networks, endangering banks' capacity to function.

Data security is a shared responsibility rather than an isolated one. India's banking industry has to prioritize client trust, strengthen its defences, and react to new dangers as it embraces digital innovation. Although the fight against cyber-attacks is still ongoing, Indian banks can traverse this challenging environment and safeguard the financial ecosystem by adopting strong cybersecurity procedures, teamwork, and awareness.

KEY RULES AND REGULATIONS

The Information Technology Act, 2000

When the I.T. Act was first introduced, its primary focus was on establishing the foundational principles of technology law, such as the recognition of digital signatures and electronic documents. The goal of giving legal legitimacy to transactions carried out electronically was stated in its preface, commonly known as electronic commerce, and enabling the electronic submission of information to government organizations. Additionally, it sought to modify current legislation like the Indian Penal Code, Indian Evidence Act, Bankers' Books Evidence Act, and Reserve Bank of India Act to accommodate the advancements in electronic communication and storage. However, it wasn't until 2008 that significant amendments were made to the I.T. Act through the Information Technology (Amendment) Act, 2008, which was effective from Oct. 2009. These amendments introduced ***S. 43A***, which required businesses to implement appropriate security measures when handling sensitive personal data and provide compensation in case of data breaches. Additionally, ***S. 72A*** was incorporated to penalize intentional breaches of personal data.

The 2008 amendments did not provide definitions for terms like personal data or sensitive personal information. Instead, S. 43A empowered the Central Government to prescribe what

constitutes $ensitive personal data through consultations with professional bodies or associations. In response to this mandate, the Central Government formulated ***the IT (Reasonable $ecurity Practices And Procedures and $ensitive Personal Data or Information) Rules, 2011***, which came into effect on March 28, 2012. These regulations, which set forth principles for the safeguarding of sensitive personal data, signalled the establishment of India's legal structure for data privacy.[1]

S. 43A of the law aims to ensure that any organization handling sensitive personal data or information takes appropriate security measures. If such an organization fails to uphold these standards and it results in harm to individuals due to negligence, it is liable to compensate those affected.

The 2011 Regulations safeguard the personal information that is gathered by an individual or by someone who engages in business or professional endeavors. This is so because all of the 2011 Rules' requirements only apply to corporations. "Any company and includes a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities" is the definition of a "body corporate" as stated in S. 43A of the I T Act. Consequently, the 2011 Rules would not apply to an individual or to someone who does not take part in commercial or professional endeavors.

The term "$ensitive personal data or information" is used frequently in the 2011 Regulations, which may give the perception that the rules are limited to sensitive data; however, closer inspection reveals that the rules also occasionally refer to "personal information or $ensitive personal data or Information," suggesting a broader scope. This is despite the fact that S. 43A specifically mentions "$ensitive personal data or information."

Rule 3 of the 2011 Regulations enumerates 8 types of personal data categorized as $ensitive personal data. These include:[2]

[1] Vinod Joseph , Protiti Basu and Ashwarya Bhargava, India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info, MONDAQ (March 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

[2] Vinod Joseph , Protiti Basu and Ashwarya Bhargava, India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info, MONDAQ (March 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

i. Passwords

ii. Financial information like bank account, credit card, debit card, or other payment instrument details

iii. Physical, physiological, and mental health conditions

iv. Sexual orientation

v. Medical records and history

vi. Biometric information

vii. Any detail pertaining to the aforementioned categories provided to a corporate body for service provision

viii. Any information received under the aforementioned categories by a corporate body for processing, storage, or lawful contractual purposes

Therefore, any information that falls into the first six classifications of sensitive personal information and is given to a business entity for the purpose of fulfilling a contract or providing services also counts as sensitive personal information.

Rule 4 of the 2011 Regulations mandates that every corporate entity, or any person acting on its behalf, who gathers, receives, holds, stores, manages, or deals with information provided by individuals, must draft a privacy policy. This privacy policy must be accessible to those individuals who have shared their information with the corporate entity under lawful contracts. Additionally, the corporate organization's webpage must provide access to the confidentiality policy. It should specify in detail the procedures and guidelines that the corporate body adheres to with regard to gathering, receiving, storing, managing, and handling information. The sorts of sensitive or personal information that the business organization collects should also be specified in the privacy policy.[3]

Rule 5 of the 2011 Regulations has a number of sub-rules pertaining to the gathering of personal information. These sub-rules apply to all forms of information as described by the IT Act, with sub-rules 1, 2, and 4 particularly addressing sensitive personal data. Prior to

[3] Vinod Joseph , Protiti Basu and Ashwarya Bhargava, *India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info*, MONDAQ (March 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

collecting any sensitive personal data, the supplier of the data must provide the collector with their approval. Furthermore, only legitimate and essential objectives may be used to gather sensitive personal data. Additionally, it is required that no business organization, or anyone working on its behalf, keep sensitive personal information longer than is necessary to fulfill legal obligations or to comply with applicable legal requirements. Rule 5's sub-rule 7 mandates that the information supplier be provided with the opportunity to revoke any permission they may have previously granted to the business entity. Sub-rule 7 seems to include all categories of personal information, but as agreement is only needed for sensitive data, it seems likely that sensitive data is the main focus of this regulation. Consent withdrawals must be made in writing to the corporate body that handled the data collection. There is no guidance on the repercussions of withdrawing permission under the 2011 Regulations. On the other hand, one may counter that a business that has personal information obtained with consent has a duty to remove it from its records when that consent is withdrawn.

According to ***Rule 6(1) of the 2011 Regulations***, any corporation that discloses $ensitive personal data to a third party must first get consent from the source of the information. A contract that outlines the parameters under which the corporate organization received the $ensitive personal data from the data source may contain this kind of prior authorization. Only sensitive personal data is covered by the aforementioned Rule 6(1) and not non-sensitive personal data.

Rules 6 and 7 of the 2011 Regulations outline a few exceptions to the general norm that requires consent before disclosing any sensitive personal information. These are the following:

- when divulgence is required to fulfill a "legal obligation".
- if government authorities request such sensitive personal information in writing in order to verify identify or to prevent, detect, investigate, including cyber incidents, prosecute, and punish offenders. The request from the government agency must be supported by a pledge to keep such private information private and confidential.
- when any third party issues an order under the already enacted legislation requiring

disclosure;[4]

Rule 7 of the 2011 Regulations permit the transferring of sensitive personal data or information, including any kind of information, to people or organizations in India or abroad but this transfer may only take place if the receiver guarantees the same degree of data security as the 2011 Rules require. Such transfers are allowed if they are required to carry out a legitimate contract between the party transferring the personal data and the person giving it, or if the person has given their agreement for the data to be transferred.

According to ***Rule 8 of the 2011 Regulations***, an organization or an individual acting on its behalf will be deemed to have adhered to reasonable security practices and procedures if they have put these standards and practices into practice and have a thorough information security program and policies in place that include operational, technical, managerial, and physical security controls appropriate for the type of business and the information assets being protected. As per Rule 8(2), the requirements for the Information Security Management System - Requirements and Security Techniques in Information Technology are met by the International Standard IS/ISO/IEC 27001, which is a standard in the field. As long as the norms of conduct recommended are "duly approved and announced by the Central Government" and "regularly validated or examined by an independent auditor who has received the proper approval from the Central Government", a body corporate may choose to adhere to standards other than IS/ISO/IEC codes of best practices for data protection. An auditor must conduct an audit of appropriate security methods and procedures at least once a year, or more frequently if the company upgrades its computer resources and processes significantly. A corporate entity will be considered to have adhered to appropriate security standards and procedures if it has adopted the IS/ISO/IEC 27001 guidelines or best practices rules for data security that have been authorized and announced by the Central Government. That is to say, Rule 8 of the 2011 Regulations establishes a safe harbor so that the body corporate can prove, in the event of an information security breach, that security control measures were carried out in accordance with their information security policies and programs, which are documented.[5]

[4] *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*, THE CENTRE FOR INTERNET AND SOCIETY, https://cis-india.org/internet-governance/files/it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf/view

[5] Vinod Joseph , Protiti Basu and Ashwarya Bhargava, *India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info*, MONDAQ (March

Reserve Bank of India (RBI) Rules and Guidelines

The fact that Indian banks reported 248 data breaches in 2022—a startling 20% of global incidents—illustrates the inadequacies of the current structure. The RBI was startled into reconsidering the banking sector's IT governance and cybersecurity structure. In October 2022, a draft of the new IT guidelines was made public. Additionally, the master directive on "Information Technology Governance, Risk, Controls and Assurance Practices" was announced by the RBI on November 7, 2023. It will go into effect on April 1, 2024.[6]

With the exception of local area banks and NBFC-core investment firms, all RBI-regulated organizations will be subject to the master directive. It lays up guidelines and a framework for managing risks, resources, performance, business continuity, and disaster recovery, as well as strategic alignment. It also includes provisions for information security policy, cyber security policy, IT and information security risk management framework, and regular assessment of hazards. The IT strategy committee of the board, the IT steering committee, and the information security committee are the three main committees that the regulated businesses are required to establish under the framework. Additionally, the regulated organizations must appoint a senior executive as their "chief information security officer" who does not report directly to the head of the IT function. Furthermore, as a business continuity precaution, it has been advised that regulated organizations do disaster recovery exercises for key information at least once every six months and back up data securely.

Previously, the commercial, financial, and credit risks were the primary concerns of the boards of regulated firms. However, as of right now, the RBI has imposed new duties on the audit committee and board of directors of regulated firms, asking them to make sure that all required precautions pertaining to information technology, information assets, business continuity, information security, and cyber security are routinely assessed. Regulatory entities' information system audits will fall under the purview of the audit committee.

It is mandatory for the regulated entity to notify the RBI, the board, senior management, customers, and CERT-In in the event of any cyber-attack. While there are no explicit criminal

19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

[6] Rashi Dhir and Trisha Shreyashi, *Masterstroke. RBI rules for cybersecurity in financial institutions*, THE HINDU BUSINESSLINE (December 17, 2023, 02:09 PM), https://www.thehindubusinessline.com/business-laws/rbi-rules-for-cybersecurity-in-financial-institutions/article67647265.ece

provisions in the guidelines, regulated companies that violate or fail to comply with the master directive shall face penalties as outlined in S. 46 of the Banking Regulation Act, 1949.

The master directive encapsulates the spirit of the Digital Personal Data Protection Act, of 2023, and aligns with the authorities' overarching goal of completely eliminating the risk of cybersecurity events and data breaches. For this reason, regulated organizations - whether internal or external - need to greatly increase their IT and cybersecurity spending.[7]

Digital Personal Data Protection Act 2023

The DPDP Bill, 2023 was presented to the Lok Sabha on 3rd August 2023, by the Minister of Electronics & Information Technology. It was subsequently approved by both the Lok Sabha and the Rajya Sabha on August 7, 2023, and on August 11, 2023, the bill received presidential assent.

The Central Government revoked the previous Personal Data Protection Bills of 2019 and 2022 due to many revisions that included significant problems with data localization, transparency, compliance requirements, etc. The aforementioned Bill was introduced following the Supreme Court's 2017 ruling in *Justice K.S. Puttaswamy Vs. Union of India*, which recognized the *"Right to Privacy"* as a component of the fundamental *"Right to Life"* guaranteed by Article 21 of the Indian Constitution. The Court also recommended that the Central Government establishes a law or policy to protect personal data.[8]

The Act's foremost objective is to control how digital personal data is processed, respect people's right to privacy protection, and acknowledge that processing and utilizing such data is necessary for legitimate purposes. The Act's wording is clear and uncomplicated, making it easy for everyone to understand. In addition, the Act strives to deliver a thorough legislative framework that would control India's digital personal data security. The Act will cover the administration of personal data in India, including data that is processed online and offline that has been digitalized. It will also include the administration of personal data outside of India

[7] Rashi Dhir and Trisha Shreyashi, *Masterstroke. RBI rules for cybersecurity in financial institutions*, THE HINDU BUSINESSLINE (December 17, 2023, 02:09 PM), https://www.thehindubusinessline.com/business-laws/rbi-rules-for-cybersecurity-in-financial-institutions/article67647265.ece

[8] Ishwar Ahuja and Sakina Kapadia, *Digital Personal Data Protection Act, 2023 – A Brief Analysis*, BAR AND BENCH (August 22, 2023, 4:00 PM), https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

that is related to the provision of products or services in India. In addition, the Act establishes a foundation for a number of additional laws that will safeguard personal data and advance India's adoption of AI and other future technologies, including the Digital India Act and other sector-specific privacy and data security regulations. Under bilateral agreements, the Act may also help Indian companies collaborate more effectively with foreign companies while protecting personal data.[9]

S. 6 of the Act stipulates that Personal Data may only be handled with the agreement of the Data Principal (person) and only for the purposes mentioned. This kind of permission must be clear, explicit, free, particular, knowledgeable, and have definite affirming measures.

Before requesting assent, the Data Fiduciary must provide a notice in compliance with ***S. 5*** that includes information about the Personal Data that will be gathered and why it will be processed. The individual whose data is being processed is free to decide otherwise at any time.

Additionally, ***S. 7*** states that such permission is not required for "legitimate uses," which comprise of the following:

(i) a specific objective for which the person willingly furnished the data;

(ii) the State providing a benefit or service, such as a subsidy, certificate, license, benefit, permits, etc.;

(iii) the State's security or the nation's sovereignty and integrity;

(iv) responding to a medical emergency, treatment, or health services;

(v) for security, as well as in the interest of maintaining public order and state security;

(vi) for employment.

The Act stipulates that a person's parent(s) or authorized guardian must offer permission on behalf of a person who is disabled or less than eighteen (18) years old. Nonetheless, pursuant

[9] Varsha Rajesh, Purushotham Kittane and Huzefa Tavawalla, *PRIVACY AND DATA PROTECTION IN INDIA: 2024 WATCHLIST AND 2023 WRAP*, NISHITH DESAI ASSOCIATES (February 02, 2024), https://www.nishithdesai.com/NewsDetails/14910

to ***S. 17(4)***, the State or any of its agencies may choose to keep Personal Data or refuse any request to have it erased.

As per ***S.s 12 to 14***, certain rights belong to the individuals whose data is being handled. These rights include the ability to:

(i) Request details about the procedure;

(ii) request that the personal data be corrected or erased;

(iii) designate rights to a substitute in the case of the principal's demise or incapacity;

(iv) seek redress for any grievances;

(v) at any point before, during, or following the processing of personal information, consent may be withdrawn.

According to ***S. 15***, Data Principals are required and obligated not to:

(i) file a frivolous or fraudulent complaint;

(ii) withhold any relevant information when supplying her Personal Data;

(iii) furnish any incorrect information or impersonate in certain situations.

A penalty according to the Act's Schedule will be imposed for failing to perform these tasks.

As per ***S. 8*** of the Act, the Data Fiduciary is required to:

(i) handle the personal information exclusively for those reasons authorized by the data principal, or for purposes for which the Data Fiduciary will assume consent (should a person neglect to notify the data fiduciary that she objects to the processing of her personal data); or for certain permissible purposes;

(ii) take appropriate steps to ascertain the accuracy and completeness of data;

(iii) put in place the necessary safeguards to secure any Personal Data that it owns or controls;

(iv) react to any correspondence from the Data Principal in order to enable her rights;

(v) in case of a personal violation, inform the concerned parties and the Data Protection Board of India.

(vi) discard Personal Data as soon as the intended use is fulfilled and legal preservation is not required (storage limits).[10]

Government agencies are not subject to data principal erasure rights or storage constraints. Any violation of the aforementioned duty must be handled in line with ***S. 33*** of the Act, as well as the Schedule thereto.

S. 16 permits the processing and transmission of personal data beyond national borders, excluding those nations that the Central Government has forbidden by notice.[11]

According to ***S. 17***, certain provisions regarding the "Obligations of Data Fiduciaries" and "Rights & Duties of Data Principal" [in Chp. 2 (except for S. 8 (1) & (5) and Chp. 3 (except S. 16) of the Act] have been declared inapplicable (exempted) in certain situations. These cases consist of but are not restricted to:

(i) the prevention, investigation, or prosecution of offenses;

(ii) the enforcement of legal rights or claims;

(iii) outside of India's borders;

(iv) processing in order to determine assets, liabilities, and financial data.

Additionally, in accordance with S. 17(2), the Act's restrictions don't apply when processing personal data:

(i) in the interest of public safety and order by the State or any of its instrumentalities;

[10] Ishwar Ahuja and Sakina Kapadia, *Digital Personal Data Protection Act, 2023 – A Brief Analysis*, BAR AND BENCH (August 22, 2023, 4:00 PM), https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

[11] Ishwar Ahuja and Sakina Kapadia, *Digital Personal Data Protection Act, 2023 – A Brief Analysis*, BAR AND BENCH (August 22, 2023, 4:00 PM), https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

(ii) required for statistical, historical, or research reasons.

In accordance with Chp. V of the Act, the Central Government is required to create the *Data Protection Board of India* (Board), which will include a chairperson and other members. The Board will carry out the duties and exercise the authority set forth in ***S.s 27 and 28*** of the Act. This includes:

(i) requiring immediate corrective or mitigating action in the event that personal data is breached,

(ii) looking into the breach, and

(iii) applying penalties in accordance with the Act.

S. 39 forbids any action or procedure relevant to any topic that the Board is empowered to consider under the Act from being heard in any other civil court. The Board shall consider complaints and cases relevant to the Act in its capacity as a civil court with original jurisdiction.[12]

The new Act requires all enterprises and firms that handle personal data to develop standard operating procedures and provide staff training to ensure compliance with certain standards. These consist of performing data protection assessments, maintaining valid contracts with data processors, hiring an Independent Data Auditor, collaborating with the Data Protection Officer designated by the Significant Data Fiduciary under S. 10 of the Act, and establishing a consent management system to collect, track, and update individual consent.

ROLE AND AUTHORITY OF REGULATING BODIES

Reserve Bank of India

The Reserve Bank of India (RBI), which serves as the nation's central bank, is essential to the oversight and control of the banking industry in India. Its power goes beyond monetary policy

[12] Ishwar Ahuja and Sakina Kapadia, *Digital Personal Data Protection Act, 2023 – A Brief Analysis*, BAR AND BENCH (August 22, 2023, 4:00 PM), https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

to include cybersecurity, privacy of data, and economic stability. Some of the measures towards data protection against breaches are as follows:

- The Reserve Bank of India (RBI) mandated regulated entities (REs) to set up strong governance frameworks and apply uniform minimum security control requirements for digital payment goods and services in their "Master Direction on Digital Payment Security Controls", which was released in February 2021. Customer protection, fraud risk management, authentication, and application security are only a few of the topics covered by the controls. Regulated Entities can safeguard consumer interests, reduce the risks connected with digital payments, and promote confidence in the digital financial ecosystem by abiding by certain restrictions.[13]

- The Reserve Bank of India (RBI) created a regulatory framework for regulated data fiduciary firms known as "Account Aggregators" in 2016. In an effort to protect consumer interests and data privacy while advancing financial inclusion and data exchange, the RBI has established a regulatory framework for account aggregators. In order to provide consumers more control over their financial information and improve the effectiveness of the provision of financial services, account aggregators are essential in enabling safe and transparent data interchange within the regulated financial system.

- By implementing policies including user access restriction, end-to-end data encryption, real-time threat detection, and vulnerability assessments, the RBI places a strong emphasis on data protection. By strengthening the security and integrity of the financial system and fostering confidence among stakeholders, these steps aid in protecting sensitive financial data against illegal access, data breaches, and cyber threats.

Preventive measures taken by the Reserve Bank of India (RBI) to safeguard data are essential to maintaining the stability and integrity of the Indian financial system. In a time of swift technological progress and growing cyber risks, the RBI's dedication to protecting consumer data from breaches is critical. Through the implementation of strong security measures like user access control, end-to-end data encryption, real-time threat detection, and vulnerability assessments, the RBI makes sure that financial institutions follow strict security guidelines,

[13] Varsha Rajesh, Purushotham Kittane and Huzefa Tavawalla, *PRIVACY AND DATA PROTECTION IN INDIA: 2024 WATCHLIST AND 2023 WRAP*, NISHITH DESAI ASSOCIATES (February 02, 2024), https://www.nishithdesai.com/NewsDetails/14910

reducing the risk of data breaches and preserving public confidence in the banking industry. In addition to safeguarding the interests of specific consumers, the central bank's proactive approach to cybersecurity and data privacy also increases the resilience of the financial system as a whole. The RBI promotes a culture of responsibility and diligence among banks and financial institutions, fostering a safe and reliable environment for performing financial transactions through the establishment of guidelines, the execution of audits, and the enforcement of regulatory compliance.[14]

Ministry of Electronics and Information Technology (MeitY).

India's digital environment is greatly influenced by the Ministry of Electronics and Information Technology (MeitY). Its duties go beyond technical infrastructure and encompass policy formation, cybersecurity, and data protection. MeitY functions under the parameters set out by the Information Technology Act of 2000. This Act establishes the legal framework for cybersecurity, e-governance, e-commerce, and electronic transactions. One of MeitY's responsibilities under this Act is to enforce the privacy and data protection clauses. MeitY actively participates in the creation of laws and policies pertaining to data protection. A few of the major projects are:

- The Digital Personal Data Protection (DPDP) Bill, attempts to improve data security and privacy in any field. The DPDP Bill, which was presented in 2022, has extensive safeguards for personal data. MeitY played a key role in the creation and improvement of this law. The Bill lays forth guidelines for consent, data processing, and breach reporting.

- The Ministry of Electronics and Information Technology (MeitY) frequently solicits public input on data protection measures via white papers and consultations. Stakeholders, including banks and financial organizations, can participate in the development of data protection rules through these interactions. MeitY encourages openness, diversity, and cooperation in the creation of data protection regulations by actively engaging stakeholders through white papers and consultations. It encourages trust, confidence, and accountability in the digital economy while empowering the

[14] Varsha Rajesh, Purushotham Kittane and Huzefa Tavawalla, *PRIVACY AND DATA PROTECTION IN INDIA: 2024 WATCHLIST AND 2023 WRAP*, NISHITH DESAI ASSOCIATES (February 02, 2024), https://www.nishithdesai.com/NewsDetails/14910

government to make well-informed choices that take into consideration the many interests and goals of stakeholders.

For India's banking industry to be resilient against data breaches, MeitY's proactive approach to data protection is essential. MeitY assists banks and other financial institutions in strengthening their defenses by actively involving stakeholders and keeping up with changing technological advancements and security risks. In the end, this proactive strategy improves public trust and financial stability by encouraging collaboration and best practices.[15]

Insurance Regulatory and Development Authority of India (IRDAI).

Data protection in India is based on the Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and $ensitive Personal Data or Information) Rules, 2011 (SPDI Rules). Understanding the need for strong data security, the IRDAI has regularly revised its recommendations to take into account new threats to the internet. In 2022, the IRDAI emphasized the necessity for thorough data protection by extending the standards' application to all insurance intermediaries.

The IRDAI released the *Information and Cyber Security Guidelines (CS Guidelines 2023) on April 24, 2023*. Applying to insurers, insurance intermediaries, and other regulated companies, these standards supersede the previous CS standards from 2017. Data-centric security, or protecting data rather than merely the network or system on which it is stored, is the main area of emphasis.

For efficient data management, regulated companies must apply a risk-based strategy in accordance with the Cyber Security (CS) Guidelines. This entails putting policies in place to lessen cyber threats and stop private client data from being lost, misused, or disclosed. It includes protecting information exchanged with staff members, outside suppliers, and business distributors. The recommendations emphasize how crucial it is to classify data based on how sensitive it is and to apply the proper levels of security for important, sensitive, and personal data. It is mandatory for regulated organizations to create comprehensive incident response strategies and guarantee timely notification of data breaches to pertinent regulatory bodies, such as the Insurance Regulatory and Development Authority of India (IRDAI). Access to data

[15] *India: Data Protection in the Financial Sector*, DATA GUIDANCE (September, 2021), https://www.dataguidance.com/opinion/india-data-protection-financial-sector

must be restricted in accordance with each person's job description inside the company. It is important to use asset management procedures to guarantee that data is handled correctly during its entire lifespan. This covers circumstances pertaining to Bring Your Own Device (BYOD) and mobile security concerns. Encryption techniques and secure networks are considered necessary to protect data confidentiality and integrity. Frequent audits are vital for evaluating adherence to the Cyber Security rules, and regulated companies must remain up to date on emerging cyber dangers in order to appropriately modify their security protocols.

The IRDAI formed an *interdisciplinary standing committee on cyber security* on September 14, 2023. The group examines current and new risks and makes recommendations for improving the cyber security posture of the insurance sector. The IRDAI's dedication to protecting policyholder data is demonstrated by its proactive approach to data protection. The Insurance and Risk Directors Association (IRDAI) is a key player in protecting the insurance industry against cyberattacks and data breaches by implementing strict regulations, raising risk awareness, and encouraging compliance. As technology advances, the IRDAI's watchfulness is still necessary to preserve security and confidence in the digital sphere.[16]

The Data Protection Board of India.

The recently passed DPDP Act 2023 established the Data Protection Board of India, marking a substantial advancement in India's data security and privacy policies. The enforcement of data protection regulations within the nation will be largely dependent on the Data Protection Board of India. It has the legal standing and power to possess property, make agreements, and bring legal action as necessary since it is a corporate organization. The Central Government will choose the site of the Board's offices, highlighting the organization's centralized approach to data security and its significance to the country.

The Central Government will appoint a certain number of members to serve on the Board, in addition to the Chairperson. The selection of these members will be predicated on their proficiency in a range of pertinent domains, including data governance, law, the digital economy, and information technology. By bringing together legal, technological, and

[16] Indranath Bishnu, *India – Primer On IRDAI Information And Cyber Security Guidelines 2023*, CONVENTUS LAW (January 9, 2024), https://conventuslaw.com/report/india-primer-on-irdai-information-and-cyber-security-guidelines-2023/

administrative viewpoints, the board's multidisciplinary structure guarantees a thorough approach to data protection.

The Board has been granted extensive jurisdiction to oversee prompt remedial measures in the event of a data breach, scrutinize complaints about breaches involving personal data, and impose penalties for transgressions of the Act. Additionally, the Board is in charge of monitoring Data Fiduciaries' and Consent Managers' adherence to their duties, underscoring the Board's critical role in defending the rights of data principals.

The Board aims to operate as a "digital office" and has a special operating structure that emphasizes digital functions. This method assures speed in resolving complaints, queries, and decision-making procedures and is consistent with the digital nature of the data it seeks to preserve.

One essential component that underpins the Board's credibility and effectiveness is its self-sufficient operation. Its independence is crucial to ensuring unbiased oversight of data security procedures in the public and commercial domains. Furthermore, the prohibition on ex-members from joining any organization they previously managed instantly enhances the Board's integrity and objectivity.

An important step in protecting personal data, increasing consumer trust in digital services, and encouraging innovation in the digital economy is the establishment of the Data Protection Board of India. Its capacity to adjust to the quickly changing digital environment and carry out its purpose effectively will determine how successful it is. As it starts up, all eyes will be on how it influences data protection procedures in India, establishing models for others to imitate in their quest for a reliable and safe digital environment.

Securities and Exchange Board of India.

The Securities and Exchange Board of India (SEBI), which is the main regulatory body overseeing the Indian securities market, is essential to maintaining data security, privacy, and industry resilience. SEBI has developed the Cyber Security and Cyber Resilience Framework specifically for Mutual Funds/Asset Management Companies (AMCs) and Stock Brokers/Depository Participants in response to the growing cybersecurity threats that securities and investment businesses are facing. These frameworks give specific guidelines for data

protection that stockbrokers, AMCs, depository participants, and Indian mutual fund companies have to follow. They use strong encryption techniques like Rivest–Shamir–Adleman (RSA) and Advanced Encryption Standard (AES) to emphasize the identification and encryption of sensitive data both in transit and at rest. Where possible, data masking techniques should also be used, and certain staff members should be in charge of maintaining encryption procedures and protecting encryption keys. Applications used by businesses that send confidential information over the internet must use secure, encrypted routes to prevent Man-in-the-Middle (MITM) attacks and prevent unwanted access. It is recommended to use transport encryption technologies such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). Furthermore, it is always advisable to hash important credentials—like passwords and security PINs—using powerful cryptographic hash algorithms before storing them in plain text.

The General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) are just a few examples of worldwide data protection standards that SEBI's laws comply with. The significance of data encryption and key management has also been emphasized by other Indian regulatory authorities, such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI), and the Unique Identification Authority of India (UIDAI). As seen by recent incidents like the punishment levied by the French data protection regulator CNIL for GDPR violations against the European online shop SPARTOO, non-compliance with data protection legislation can carry significant costs.

SEBI promotes the use of strong incident response plans, strict password policies, and data loss prevention (DLP) systems. Its proactive approach demonstrates how committed it is to maintaining security, integrity, and trust in the Indian securities market. SEBI's watchfulness is essential to protecting sensitive financial data from any breaches as technology develops. In addition, SEBI is strengthening its cybersecurity defences by designating a Chief IT Security Officer to manage programs designed to protect the market from cyberattacks.[17]

[17] Varsha Rajesh, Purushotham Kittane and Huzefa Tavawalla, *PRIVACY AND DATA PROTECTION IN INDIA: 2024 WATCHLIST AND 2023 WRAP*, NISHITH DESAI ASSOCIATES (February 02, 2024), https://www.nishithdesai.com/NewsDetails/14910

PENALTIES

The penalties for data breaches in India under various relevant laws are as follows:

Digital Personal Data Protection Act, 2023.

The Act's Schedule lists the fines that will be imposed for certain violations and infractions. Among these sanctions are:

- INR 200 crore as a fine for breaking commitments pertaining to children.
- According to ***S. 8(5)*** of the Act, there is a penalty of INR 250 crore for failing to put security measures in place to avoid data breaches.
- Failure to inform the Board or the Data Principal of a breach involving personal data as required by ***S. 8(6)*** of the Act may result in a penalty of INR 200 Crore.

After an investigation is carried out in accordance with S. 33 of the Act, the Board shall be enforcing these sanctions.[18]

The Information Technology Act, 2000.

The ***2011 Rules*** do not specify any penalties for violations of their provisions.

The IT Act's ***S. 72A*** deals with the disclosure of personal information without authorization, which is illegal and can result in a fine of up to five lakh rupees, three years in prison, or both. Certain conditions must be satisfied in order for a breach of this provision to be considered unlawful, such as obtaining access to personal data through a legitimate contract, revealing the data with the aim to harm or profit, getting consent from the individual in question, or breaking the terms of the contract safeguarding the data. Crucially, culpability does not need actual loss or damage arising from the disclosure; rather, liability is based only on the intention to cause injury or advantage.

[18] Ishwar Ahuja and Sakina Kapadia, *Digital Personal Data Protection Act, 2023 – A Brief Analysis*, BAR AND BENCH (August 22, 2023, 4:00 PM), https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

Even in situations when deliberate failure to maintain appropriate security standards and procedures occurs, ***S. 43A*** does not entail criminal sanctions; instead, it demands compensation for carelessness on the part of a body corporate.[19]

Reserve Bank of India Rules and Guidelines.

In the financial industry, the RBI is a major regulator of data protection. The RBI may impose fines for violations involving loan applications, payment aggregators, and other financial services. The seriousness of the violation and non-compliance with RBI standards determine the specific penalty amounts.[20]

CONCLUSION

In conclusion, the Indian banking industry has a strong and dynamic regulatory framework for handling data breaches that safeguard private client information. A dedication to cybersecurity is shown by actions like risk-based strategies, incident response plans, and encryption methods. Notwithstanding, certain obstacles persist, such as the dynamic character of cyberattacks and the requirement for ongoing attentiveness. Establishing a culture of cybersecurity awareness requires cooperation between financial institutions, regulatory agencies, and other relevant parties. The Indian banking industry can improve confidence and stability in the digital era and guarantee the security of clients' financial information by placing a high priority on data protection and investing in cybersecurity infrastructure.

[19] Vinod Joseph , Protiti Basu and Ashwarya Bhargava*, India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info*, MONDAQ (March 19, 2020), https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

[20] Rashi Dhir and Trisha Shreyashi, *Masterstroke. RBI rules for cybersecurity in financial institutions*, THE HINDU BUSINESSLINE (December 17, 2023, 02:09 PM), https://www.thehindubusinessline.com/business-laws/rbi-rules-for-cybersecurity-in-financial-institutions/article67647265.ece